AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: /S Bow Bottomly 06/18/2025

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of
PROPERTY KNOWN AS:
8555 N Dobbs Rd
Harrah, OK 73045

Case No: M-25-402-STE

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. § 2252A(a)(2)	Distribution of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Marisol Flores, Federal Bureau of Investigation, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

Marisol Flores
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: Jun 18, 2025

Judge's signature

City and State: Oklahoma City, Oklahoma

SHON T. ERWIN, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Marisol Flores, a Special Agent with the Federal Bureau of Investigation (FBI), Oklahoma City, Oklahoma, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) since May 2015, and I am currently assigned to the Oklahoma City Division. I am currently assigned to investigate violations of federal law involving the exploitation of children. I have gained expertise in conducting such investigations through everyday work in my current role as an SA with the FBI.

2. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. The information contained in this Affidavit is based upon my personal knowledge and observation, my training, conversations with other law enforcement officers, and review of documents and records. This Affidavit is made in support of an application for a warrant to search the entire premises located at 8555 N Dobbs Rd., Harrah, Oklahoma 73045 (hereinafter referred to as "the **SUBJECT PREMISES**"), which is described in detail in Attachment A to this Affidavit, including the residential dwelling, vehicles, curtilage, any persons located on said property, and any computer (as broadly defined in 18 U.S.C. § 1030(e)(1)) or other digital file storage device located there, for the items specified in Attachment B hereto, which constitute instrumentalities, fruits, and evidence of violations 18 USC § 2252A (possession and distribution of child pornography).

4. This investigation, described more fully below, has revealed that an individual named Shawn Michael Marlow, between on or about January 13, 2025, and March 20, 2025, who has resided at the **SUBJECT PREMISES** since at least 2020, knowingly utilized Kik to possess

and distribute child pornography, to distribute, and possess, in violation of 18 U.S.C. § 2252A, and that there is probable cause to believe that evidence, fruits, and instrumentalities of such violations are located at the **SUBJECT PREMISES**.

5. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

TERMS

6. Based on the training and experience of other law enforcement officers with whom I have had discussions I use the following technical terms and definitions:

a. An Internet Protocol (IP) address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static, or long-term, IP addresses. Other computers have dynamic, or frequently changing, IP addresses.

b. Internet Service Providers (ISPs) as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

c. Computer, as used broadly herein, refers to "an electronic, magnetic,

optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones. See 18 U.S.C. § 1030(e)(1).

d. Minor as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

e. Records, documents, and materials as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT RECEIVE OR DISTRIBUTE CHILD PORNOGRAPHY

7. Based on the training and experience of other law enforcement officers with whom I have had discussions and my own research, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

a. Individuals with intent to view or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals with intent to view or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children

oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with intent to view or possess, collect, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain photos, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals with intent to view or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals with intent to view or possess, collect, receive, or distribute child pornography also may correspond with or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access online forums,

such as bulletin boards, newsgroups, internet relay chat or chat rooms are considered more advanced users and therefore more experienced in acquiring and storing a collection of child pornography images.

8. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND OF INVESTIGATION

9. On March 14, 2025, at 20:41:22 UTC, Media Lab/Kik Electronic Service Provider submitted a CyberTip to the National Center for Missing and Exploited Children (NCMEC) regarding Kik Username: smh2022_c3t communicating with another Kik user how smh2022_c3t sexually abused their younger sister. Media Lab/Kik provided the following information to NCMEC:

Name: Shawn Me

Address: Fort Smith, AR US

Date of Birth: 08-05-1992

Email Address: shawn.marlow2020@gmail.com

All email addresses reported? Yes

ESP Product/Service: Kik

Screen/User Name: smh2022_c3t

Display Name: smh2022

ESP User ID: smh2022_c3t

Compromised Account? No

IP Address: 12.75.0.97 03-13-2025 17:30:00 UTC

Estimated Location: Fort Smith, Arkansas, US at 03-13-2025 17:30:00 UTC

10. Media Lab/Kik described in their information to NCMEC the above user communicated the following to another user in a private chat on January 13, 2025, 02:23:27.014000 UTC:

"I started eating my sisters pussy when she was 6 and I was 13 she sucked my dick and swallowed my cum first time and 6 months later"

11. On March 28, 2025, at 09:10:32 UTC, Media Lab/Kik Electronic Service Provider submitted a CyberTip to the NCMEC regarding Kik Username: smh2022 distributing pornography to another Kik user in a private chat. Media Lab/Kik provided the following information to NCMEC:

Kik Messenger

Email Address: shawn.marlow2020@gmail.com

ESP Product/Service: Kik

Screen/User Name: smh2022

Display Name: Shawn Me

ESP User ID: smh2022_c3t

Media Lab/Kik described in their information to NCMEC the above user uploaded a video and an image to another user in a private chat. Those files are described in the following paragraphs.

12. The video file, 2c9d6ba1-58ef-4c88-93e3-1dc50690367c.mp4, was

uploaded on March 20, 2025, at 13:26:14 UTC. This video was one minute and forty seconds in length. The video depicted a prepubescent female, whose face was visible from the camera view, with a pink, short sleeve shirt on. The prepubescent female was performing oral sex on a pubescent female of an indeterminate age, who was naked from at least the waist down. The prepubescent female continues to perform oral sex on the other female while the other female is both standing and sitting throughout the video.

13. The image file, 4eb0c4de-cb4a-432c-95a5-60bcf03e383a.jpg, was uploaded on March 20, 2025, at 13:24:44 UTC. This image depicted a prepubescent female lying on her back, naked from her chest down exposing her breast area and vagina. Standing next to the child is an adult male visible from the waist down with an erect penis. The prepubescent female is holding the adult male's erect penis with both of her hands.

14. On March 26, 2025, an administrative subpoena was served to Kik, through its parent company MediaLab.ai. On May 3, 2025, Kik, through its parent company MediaLab.ai, provided information regarding email address: shawn.marlow2020@gmail.com; screen/user name: smh2022_c3t; display name: smh2022; ESP User ID: smh2022_c3t pursuant to an administrative subpoena served on March 26, 2025. The following is a portion of the information provided by Kik:

Date: May 3, 2025

First Name: Shawn

Last Name: Me

Email: shawn.marlow2020@gmail.com

Username: smh2022

Login IP: 70.182.93.83 52886 2024-10-13 16:58:45 CAN

Login IP: 70.182.71.46 59740 2024-11-10 18:00:02 CAN

Login IP: 70.182.71.46 53556 2025-02-16 18:01:00 CAN

15. On March 26, 2025, an administrative subpoena was served to Google Inc. to provide information pertaining to email address: shawnmarlow2020@gmail.com. On March 26, 2025, Google Inc. responded with the following information:

Google Subscriber Information

Google Account ID: 762897971482

Name: Shawn Marlow

Given Name: Shawn

Family Name: Marlow

E-Mail: shawn.marlow2020@gmail.com

Created on: 2018-08-28 21:32:13 Z

Account Recovery

Recovery SMS: +14059683540 [US] = T-Mobile

Postal Address

Created on: 2018-11-20 21:35:34 UTC

Postal Code: 73106

Locality Name: Oklahoma City

Address Line: 1729 Northwest 3rd Street

Recipient Name: Shawn Marlow

Phone Number Saved to Address: + 1 405-446-6174

Postal Address

Created on: 2019-11-10 14:07:59 UTC

Postal Code: 73045

Locality Name: Harrah

Postal Code

Address Line: 9633 North Harrah Road

Recipient Name: Shawn Marlow

16. Based on open-source records, it was determined IP addresses 70.182.71.46 and 70.182.93.83 were controlled by Cox Communications. On or about May 6, 2025, an administrative subpoena was served to Cox Communications to provide information pertaining to Kik Login IP addresses: 70.182.93.83 on 2024-10-13 16:58:45 UTC Port 52886 and 70.182.71.46 on 2024-11-10 18:00:02 UTC Port 59740, and 2025-02-16 18:01:00 UTC Port 53556. On or about May 12, 2025, Cox Communications responded with the following regarding both IP addresses:

Name: Nowakoski LLC DBA Tubs of Sud

Address: 3400 S Harrah Rd Harrah, OK 73045-6078

Telephone number: 405-637-5331

17. On April 9, 2025, an administrative subpoena was served to T-Mobile USA, provide information pertaining to telephone number: 405-968-3540. On or about April 22, 2025, T-Mobile USA, Inc. responded with the following information:

Subscriber Name: Ashley Livengood

Subscriber Address: 12629 NE 39th St., Spencer, OK 73084

Subscriber Status: Active

Activation Date: 08/15/2022

18. Open-source checks for Shawn Marlow show an address of 8555 N Dobbs Rd., Harrah, Oklahoma. One of two phone numbers listed for Shawn Marlow from January 2020 to January 2025, is 405-968-3540, the same number associated with the Google email described in paragraph 11. The other listed phone number is 405-827-0865. In addition, a financial record revealed Shawn Marlow with a financial transaction on January 17, 2025. This recorded listed his associated phone number as 405-968-3540, and his associated address as 8555 N Dobbs Rd, Harrah, OK 73045-8873.

19. The Oklahoma Sex Offender Registry lists Shawn Michael Marlow, date of birth August 5, 1992, as a registered sex offender as of August 7, 2017, with a completion of sentence of March 2, 2026. Marlow's listed alias is Shawn Michael Heuer. There are two crimes listed from Osage County, Soliciting Sexual Conduct of Communication with Minor by use of Technology and Asst Lewd Exhibition, both of which have conviction dates of March 3, 2017. The home address for Shawn Marlow on the Oklahoma Sex Offender Registry is 8555 N Dobbs Rd, Harrah, Oklahoma 73045. The Employers listed is TAKE TEN TIRE at 1330 S. Eastern, Oklahoma City, Oklahoma. Shawn Marlow's vehicle listed on the Oklahoma Sex Offender Registry is a dark blue Dodge Ram 1500 (Pickup) with Oklahoma license plate QBW431. On February 14, 2025, the Oklahoma Department of Corrections has a record of Shawn Marlow's Sex Offender Registration and Notice of Duty to Register, with Marlow's address of 8555 N Dobbs Rd., Harrah, Oklahoma 73045, and a primary phone number of 405-827-0865.

20. The vehicle registration for Oklahoma license plate QBW431 checks back to a 2018 Dodge Ram 1500, gray in color, vehicle owner of Shawn M Marlow at 8555 N Dobbs Rd, Harrah, OK 73045873.

21. On June 11, 2025, law enforcement observed the 2018 Dodge Ram 1500 with Oklahoma license plate QBW431, at Take Ten Tire, 1330 S. Eastern, Oklahoma City, Oklahoma, Shawn Marlow's listed employment.

22. On June 16, 2025, law enforcement observed the 2018 Dodge Ram 1500 with Oklahoma license plate QBW431, at Take Ten Tire, 1330 S. Eastern, Oklahoma City, Oklahoma, Shawn Marlow's listed employment.

23. Based on my training and experience, and the facts presented thus far, I believe Shawn Marlow used Kik Usernames: smh2022_c3t and smh2022 to possess and distribute child pornography.

24. On or about June 16, 2025, a search warrant was served to Kik for both usernames, smh2022_c3t and smh2022, and on June 17, 2025, a search warrant was served to Google for email address shawn.marlow2020@gmail.com. Those returns and review of returns are pending. On June 18, 2025, a search warrant was executed on Marlow's person and a search warrant was executed on his vehicle, the 2018 Dodge Ram 1500 with Oklahoma license plate QBW431, at Take Ten Tire, 1330 S. Eastern, Oklahoma City, Oklahoma. A Samsung Galaxy S24 cell phone was seized on Marlow's person. During a live preview of the cell phone, the Kik application was observed. The Kik account information on the cell phone revealed a username: smhe2, email: smhe202@yahoo.com, and name: smhe2. The cell phone device phone number was 405-642-8743, and the

Google Mail application contained an email address of smhe202@gmail.com. One of the SMS text messages observed between Marlow and an unknown individual on August 5, 2024, contained the following:

> Marlow texts, "Ive always wanted to have a mother and daughter together lol …Yea would be so hot … Would you ever have a 3 way with your daughter". The other individual texts, "Noooooo".

25. Your affiant conducted postal checks and it was confirmed that Marlow receives mail at 8555 N Dobbs Rd., Harrah, Oklahoma 73045, **SUBJECT PREMISES**. Marlow's current vehicle has a registration with his name and listed address 8555 N Dobbs Rd., Harrah, Oklahoma 73045, **SUBJECT PREMISES.** Oklahoma Department of Corrections Probation has had numerous visits to Marlow's residence at 8555 N Dobbs Rd., Harrah, Oklahoma 73045, **SUBJECT PREMISES,** since December 16, 2019, to April 8, 2025[1]. During the execution of the search warrants described above, law enforcement conducted a custodial interview of Marlow in which he stated he has rented and lived at 8555 N Dobbs Rd., Harrah, Oklahoma 73045, the **SUBJECT PREMISES**, since 2020[2]. Also, during the custodial interview, Marlow stated the phone number to the device law enforcement seized was 405-827-0865, and he has had this phone for approximately six months. Marlow added he has a PlayStation at his house. When asked how come the cell phone law enforcement seized did not match the phone number provided, Marlow stated that phone was at his house.

26. Based on my training and experience, individuals who possess and distribute child

[1] Department of Corrections Probation Officer managing Marlow's case stated she has had multiple visits at the **SUBJECT PREMISES** and described it as a single level, trailer on a property.
[2] Marlow stated his residence has two bedrooms.

pornography store and share files on multiple digital devices. PlayStation consoles, depending on the model, can store image and video files, as well as share files. I also know there is at least one additional cell phone at Marlow's residence that might have been used to store and share files. I believe Marlow has and is storing child pornography on other digital devices based on the above information, and I am seeking authority to search the **SUBJECT PREMISES** for additional evidence of possession and distribution of child pornography by Marlow.

BACKGROUND ON DIGITAL MEDIA STORAGE DEVICES AND CHILD PORNOGRAPHY

27. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Other digital media storage devices (e.g., compact disks, digital video disks, floppy disks, cell phones, Blackberries, iPhones, thumb drives, video gaming stations, etc.) can also store tremendous amounts of digital information, including digital video and picture files.

28. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. Further, even if deleted, forensic examination can sometimes recover files and data including

deleted picture files.

29. Computers and other digital file storage devices can store the equivalent of thousands of pages of digital information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires the searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks depending on the volume of the data stored, and it would be generally impossible to accomplish this kind of data search on site. Furthermore, I know that smart cell phones (a type of "computer," as broadly defined in 18 U.S.C. § 1030(e)) can typically "synch" with a traditional desktop or laptop computer. The purpose of synching a smart phone to a traditional computer is to back up data that is stored on the phone so that it is not permanently lost if the portable smart phone is lost or damaged. Also, smart phone users may move files off the smart phone and onto a computer to free up storage space on the smart phone. Similarly, computer (e.g., desktop computers, smart phones, etc.) users may move files off one computer and onto another computer or a digital file storage device such as a thumb drive, a DVD, or an external hard drive, to free up space on the computer. For this reason, I am seeking authorization to seize all computers and digital file storage devices at the **SUBJECT PREMISES**—not any particular computer.

SPECIFICS OF SEARCH AND SEIZURE OF CELL PHONES AND COMPUTER SYSTEMS

30. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment.

This is almost always true for the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all of the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

31. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child exploitation where the evidence frequently includes graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition,

the analyst needs all of the system software (operating systems or interfaces, and hardware drivers) and any application software which may have been used to create the data (whether stored on hard drives or on external media).

32. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

33. The search procedure for electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. searching for and attempting to recover any deleted, hidden, or encrypted

data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offense specified above);

e. surveying various file directories and the individual files they contain;

f. opening files in order to determine their contents;

g. scanning storage areas;

h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

SMARTPHONES AND PLAYSTATION

34. Finally, based on the training and the experience of other law enforcement officers and my own research, I know that people who use their computers (including smartphones and Playstations) to view/access/possess child pornography do so in private to avoid detection. I also know that people who view/access/possess child pornography often use their smartphone and Playstations. I know smartphones and Playstations can transfer files back and forth with other computers and digital file storage devices. Files can be stored simultaneously on multiple computers or other digital file storage devices. Marlow has stated that he has at least one cell phone and one Playstation at the **SUBJECT PREMISES.** I believe there is probable cause that his cell phone and Playstation, other computer(s), and other digital

file storage device(s) will contain evidence of the aforementioned criminal violations, as outlined in detain in Attachment B.

EXECUTION TIME OF THE WARRANT

35. MARLOW has been arrested as based on his statements no one else lives at the SUBJECT PREMISES. I am requesting that the search warrant authorize execution in the daytime between 6:00 a.m. to 10:00 p.m.

CONCLUSION

36. Based on the above information, there is probable cause to believe that the foregoing laws have been violated, and that the following property, evidence, fruits, and instrumentalities of these offenses are located at the **SUBJECT PREMISES**.

37. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the **SUBJECT PREMISES**, described in Attachment A, authorizing the seizure of the items described in Attachment B to this Affidavit.

Marisol Flores
Special Agent
Federal Bureau of Investigation

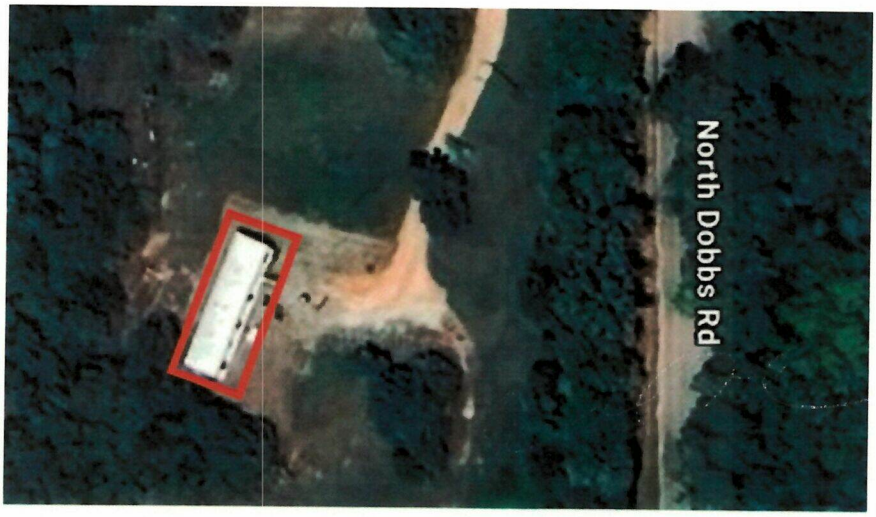
SUBSCRIBED AND SWORN to before me this 18th day of June 2025.

SHON T. ERWIN
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PREMISES

8555 N Dobbs Rd, Harrah, OK 73045 is located within the Western District of Oklahoma. The SUBJECT PREMISES is a single-family, single-story dwelling. The subject premises is a two bedroom trailer home. The mailbox on the street in front of the entrance to the SUBJECT PREMISES has the digits 8555.



ATTACHMENT B
LIST OF ITEMS TO BE SEIZED AND SEARCHED

Contraband, evidence, fruits, and instrumentalities related to Shawn Michael Marlow distributing child pornography in violation of 18 U.S.C. § 2252A(a)(2) or possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), in any form, including, but not limited to:

1. All records, including those stored digitally, to the extent they are reasonably believed to belong to or be used by Shawn Marlow, pertaining to the distribution, or possession of child pornography, as defined in 18 USC 2256(8), or to the distribution, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 USC 2256(2), including:

   a. Records and information relating to images or videos of suspected child pornography;

   b. Records and information relating to communications between individuals about child pornography;

   c. Records and information relating to the existence of sites on the internet that contain child pornography or that cater to those with an interest in child pornography;

   d. Records and information relating to membership in online groups, clubs, or services that provide or make accessible child pornography to members;

   e. Records and information relating to any e-mail accounts used to view, access, trade or distribute child pornography;

   f. Records and information relating to malicious software;

2. To the extent they are reasonably believed to belong to or be used by Shawn Marlow: computers or storage media used as a means to commit the violations described above. This includes video game consoles such as Playstation or Xbox.

3. To the extent they are reasonably believed to belong to or be used by Shawn Marlow: Routers, modems, and network equipment used to connect computers to the Internet.

4. To the extent they are reasonably believed to belong to or be used by Shawn Marlow: any and all cameras, film, videotapes or other photographic equipment capable of storing images or videos of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all visual depictions of minors to see if they match images of minors in child pornography.

6. To the extent they are reasonably believed to belong to or be used by Shawn Marlow: any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the vehicle described above, including, but not limited to, rental or lease agreements, purchase documents, rental or lease payments, registration paperwork, mail envelopes, or addressed correspondence.

7. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the

COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer", as broadly defined in 18 U.S.C. § 1030(e), includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.